金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

# 109 年度主要檢查缺失

## -專營電子支付機構

# 目　　次

## 業務項目：防制洗錢、打擊資恐及反武擴作業

**缺失態樣**

**辦理防制洗錢及打擊資恐查詢資料庫之建檔，有欠完整。**

**缺失情節**

- 自建防制洗錢及打擊資恐資料庫名單欠完整，如：國際制裁人物黑名單僅建置身分證字號、中文姓名及「護照英文姓名」，未建置「使用之英文姓名」及與其相關法人。
- 辦理國內重要政治人士資料建檔，未完整建置「家庭成員」及「有密切關係之人」資料。
- 對警政單位通報為涉及詐騙之案關會員，未納入資料庫負面新聞之名單內，並重新評估風險等級。

**改善作法**

- 應完整建置防制洗錢及打擊資恐查詢資料庫，並訂定資料庫建檔作業程序及審核規範，定期辦理檢視，以落實客戶身分審查。

## 業務項目：業務操作管理

**缺失態樣**

**辦理使用者申請註冊及開立電子支付帳戶之檢核驗證機制，有欠妥善。**

**缺失情節**

- 對於不同會員使用同一金融支付工具作為身分確認，未建立相關檢核管控機制，以拒絕其註冊申請。

**改善作法**

- 應參照「電子支付機構使用者身分確認機制及交易限額管理辦法」第 5 條第 1 項第 6 款規定，「對於已提供用於身分確認之同一金融支付工具，遭不同使用者重複提供用於身分確認，應拒絕其註冊申請」。

## 業務項目：業務操作管理

**缺失態樣**

**辦理電子支付帳戶使用者身分確認作業，有欠妥適。**

**缺失情節**

- 接受使用者註冊申請帳戶，未向金融聯合徵信中心查詢「使用者通報案件及加強身分確認註記資訊」(P33)。
- 接受使用者註冊及開立第二類及第三類帳戶，未向金融聯合徵信中心查詢「使用者國民身分證領換補資料查詢驗證」(P11)。

**改善作法**

- 應參照「電子支付機構使用者身分確認機制及交易限額管理辦法」第 4、8、9 及 10 條規定辦理：
  - 電子支付機構接受使用者註冊申請時，應向金融聯合徵信中心查詢疑似不法或顯屬異常交易存款帳戶資料及加強身分確認註記資料，並留存相關紀錄備查。
  - 電子支付機構接受個人使用者註冊及開立第二類及第三類帳戶，應向金融聯合徵信中心查詢國民身分證領換補資料之真實性。

## 業務項目：資訊安全管理

**缺失態樣**

**辦理防火牆規則檢視作業有未落實，或規則設定欠嚴謹。**

**缺失情節**

- 雖已定期檢視防火牆安全規則，惟未將高風險性網路通訊服務埠，如：檔案傳輸(FTP)、遠端桌面（RDP）、遠端登入(TELNET)及重要連線所採SSH(Secure Shell)遠端登入協定等納入檢視重點。
- 防火牆所設定之連線有逾半年以上流量為零，而未評估處理。
- 防火牆規則設定過於寬鬆，如：對非武裝區(DMZ)之伺服器開啟無必要使用之域名解析服務(DNS)。

**改善作法**

- 應妥適訂定防火牆規則定期檢視之重點項目，依最小授權原則落實辦理檢視作業，並刪除非必要之網路連線。

## 業務項目：資訊安全管理

**缺失態樣**

**對外服務網站安全防護作業，有欠妥善。**

**缺失情節**

- 官網對用戶端瀏覽器之設定，未採用安全標頭(Headers)設計，如：未採用 Strict-Transport-Security 強化網頁瀏覽機制、Content-Security-Policy 防禦跨網站指令攻擊、X-Frame-Options 防禦內嵌惡意網頁攻擊、X-Content-Type-Options 避免瀏覽器誤判文件格式、Referrer-Policy 保護資訊洩漏及 Feature-Policy 管控特定應用程式介面(API)或瀏覽器功能等安全標頭(Headers)，不利防範網路攻擊。
- 官網接受 TLS 1.11 不安全加密方式風險弱點，可能導致攻擊者進行中間人攻擊，解密網站伺服器與使用者間通訊。

**改善作法**

- 應建立定期檢視對外服務網站安全機制，以維資訊安全。

## 業務項目：資訊安全管理

**缺失態樣**

**對所蒐集資安情資或警訊通報之處理作業，有欠妥適。**

**缺失情節**

- 未訂定資安情資或警訊通報處理之標準程序或作業規範。
- 對所蒐集之資安情資未妥善處理，且未留存評估、處理等相關作業紀錄，如：對金融資安資訊分享與分析中心(F-ISAC)提供資安情資之惡意網域清單，未納入入侵防護系統(IPS)管控。

**改善作法**

- 應訂定資安情資或警訊通報處理之標準作業程序或規範，並留存評估及處理相關作業紀錄，以強化安全防護措施。